IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

J.B. AND M.B., minors, by and through their legal guardian Patrick Bowler, Individually and on behalf of all others similarly situated,

Plaintiffs,

v.

POWERSCHOOL HOLDINGS, INC.

Defendant.

CLASS ACTION COMPLAINT

Case No.: _____

JURY TRIAL DEMANDED

TABLE OF CONTENTS

CLASS ACTION COMPLAINT

Plaintiffs J.B. and M.B. (collectively "Plaintiffs"), minors, by and through their legal guardian, Patrick Bowler, on behalf of themselves and all others similarly situated (the "Class Members"), by and through their undersigned attorneys, bring this Class Action Complaint against Defendant PowerSchool Holdings, Inc. ("PowerSchool" or "Defendant"), and allege, upon personal information and belief and the investigation of their counsel,[1] that PowerSchool failed to safeguard highly sensitive personally identifiable information ("PII") of students, teachers, and other individuals, including minors, using PowerSchool products, including their name, social security number ("SSN"), demographic information, date of birth, phone number, email address, and medical information, and were damaged thereby.

Plaintiffs and Class Members entrusted Defendant PowerSchool with their highly sensitive PII and reasonably expected that PowerSchool would safeguard their PII at least in accordance with PowerSchool's representations. PowerSchool knew the sensitive PII it maintained is the type of information highly sought after by hackers. With this knowledge, PowerSchool assured its customers, that all user data PowerSchool retained or collected would be kept safe. For this reason, PowerSchool knew or should have known that reasonable measures must be employed to protect Plaintiffs' and Class Members' highly sensitive PII from unauthorized disclosure. PowerSchool failed to fulfill that responsibility in December 2024 when PowerSchool permitted a serious system vulnerability to arise and be exploited, resulting in the massive Data Breach. Since exposing thousands of students' and teachers' PII to hackers, PowerSchool has further failed to timely and properly notify Plaintiffs and Class Members. To

[1] Plaintiffs' counsel is engaging in an active investigation into the data breach referenced in ¶¶8-18 (the "Data Breach").

date, PowerSchool has not notified the affected individuals. As a result of PowerSchool's misconduct, Plaintiffs and Class Members have suffered and will continue to suffer damages.

INTRODUCTION[2]

1. Defendant PowerSchool is one of the nation's leading providers of cloud-based education software for school administrators. Headquartered in Folsom, California, PowerSchool has an estimated 18,000 customers worldwide, including schools and school districts ranging from kindergarten to twelfth grade levels.[3]

2. As part of offering educational software services, PowerSchool is responsible for collecting, managing, and safeguarding the PII of at least fifty (50) million students within the United States along with the PII of teachers, staff, and family members.

3. According to its website, PowerSchool offers a variety of EdTech software products which allow schools to manage a variety of administrative tasks ranging from enrollment to curriculum and teacher recruitment.

4. One product, central to PowerSchool's offerings, is its PowerSchool Student Information System ("SIS"). PowerSchool touts this software product as: "one ***secure*** customizable platform providing the interoperability need to power your school and district operations with accurate student data."[4] Notably, the PowerSchool SIS product is not limited to gathering and maintaining student data alone; it also allows for "gather[ing] ***vital information*** from families and staff."[5]

---

[2] All emphasis throughout is added.

[3] *PowerSchool data breach exposes millions of student and teacher records*, Fox News (Jan. 12, 2025 10:00 am), https://www.foxnews.com/tech/powerschool-data-breach-exposes-millions-student-teacher-records?msockid=09342d2fc1336530353f3ec7c05464fd.

[4] *PowerSchool SIS at-a-glance*, PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis/#video (last visited Jan. 17, 2025).

[5] *Id.*

5. As evidenced by PowerSchool's repeated public representations to the market, PowerSchool understood the highly sensitive nature of the PII it was gathering and maintaining. This highly sensitive PII includes: names, email addresses, phone numbers, social security numbers, medical information (*e.g.*, food allergies and learning disabilities), dates of birth, reduced meal statuses (*i.e.*, financial information), demographic information, and student and staff identification numbers.

6. As a condition of receiving education services, Plaintiffs J.B., M.B., and Class Members who were students, including their families, were required to enter highly sensitive PII which touched on every aspect of their personal lives.

7. Given the sensitivity of the PII being collected, and PowerSchool's repeated representations, PowerSchool had an obligation to safeguard the highly sensitive PII of its users, including students, teachers, and their families. However, PowerSchool failed to fulfill that obligation.

8. On or about December 19, 2024, PowerSchool experienced a breach of its SIS system as a result of a vulnerability (the "Data Breach"). Specifically, one or more unauthorized parties were able to gain access to PowerSchool's systems and data by accessing and using compromised credentials. Worse, developing evidence suggests that these parties may have gained access to PowerSchool's SIS system even earlier than December 19, 2024.

9. PowerSchool failed to discover its network vulnerability and the unauthorized access to its systems until December 28, 2024.

10. Recent reports indicate that PowerSchool failed to implement and/or improperly configured a multi-factor authentication ("MFA") protocol to ensure effective authentication and

access security. At a minimum, MFA—widely recognized as a necessary best practice—could have flagged or prevented unauthorized third party access through compromised credentials.

11. As a result of PowerSchool's failure to implement proper protocols and prevent unauthorized access, unauthorized third party hackers were able to access troves of PII of its users, including students, teachers, and their families. Hackers were able to amass and export the stolen data into a .CSV file.

12. According to news reports and other sources, in the days that followed, these hackers threatened to make the stolen data public unless PowerSchool agreed to pay a ransom. PowerSchool is suspected to have paid the ransom. There is no evidence or confirmation that the unauthorized third parties deleted any stolen data as a result of the suspected ransom payment. Further, there is no evidence that PowerSchool took steps to ensure that students' and teachers' PII was, in fact, deleted.

13. As a result of PowerSchool's negligent and/or reckless data retention, the highly sensitive PII of current and former user data from schools across the United States was accessed, viewed, downloaded, and stolen by unauthorized parties. The data stolen dates back to 2005.

14. To date, PowerSchool has failed to provide timely notice of the Data Breach to Plaintiffs and Class Members. Indeed, PowerSchool failed to notify the impacted schools until at least January 7, 2025, and, in most cases, January 9, 2025—**nearly two (2) weeks after PowerSchool learned of the Data Breach.**

15. In addition to untimely notice, PowerSchool has also failed to provide sufficient notice of the Data Breach. Specifically, PowerSchool has failed and continues to fail to provide information necessary to assess the full impact of the breach including who or which unauthorized third parties gained access its systems, exactly how long the breach lasted,

precisely what data was accessed, viewed, downloaded, and stolen, the terms of PowerSchool's ransom payment, and whether the stolen data has been or will be deleted.

16. Because of PowerSchool's negligent and/or unreasonable cybersecurity protocols and untimely notice of the Data Breach, Plaintiffs and Class Members face an imminent risk of identity theft and fraud. In fact, Plaintiffs and Class Members may already be suffering from identity theft and fraud, but cannot take steps to mitigate any harm because of PowerSchool's failure to provide proper notice.

17. Now, Plaintiffs and Class Members are forced to take affirmative steps to protect themselves against the imminent risk of identity theft or fraud that they would not otherwise have to take, such as (i) implementing credit freezes; (ii) setting alerts with credit reporting agencies; (iii) alerting financial institutions; (iv) closing or modifying bank accounts; or (v) monitoring credit reports for unauthorized activity.

18. Finally, Plaintiffs and Class Members face the risk of further unauthorized exposure of their PII because PowerSchool has not explained precisely what steps, if any, it has taken to correct the security vulnerability to prevent additional breaches. Nonetheless, PowerSchool maintains possession, custody, and control over some of Plaintiffs' and Class Members' most sensitive PII. Plaintiffs and Class Members will not (and cannot) receive any such confirmation until PowerSchool completes its investigation.

PARTIES

19. Plaintiff J.B. ("Plaintiff J.B.") is a minor resident and citizen of the State of New York and a student of Lynbrook High School, an institution that relied on Defendant PowerSchool to manage the PII of its students and teachers. Plaintiff J.B. used PowerSchool products for education services, and provided highly sensitive PII to PowerSchool in order to receive education services. Plaintiff J.B. provided highly sensitive PII based on the reasonable

assumption that PowerSchool would secure and safeguard PII with adequate security and privacy measures and protect PII from unauthorized disclosure and as a condition of receiving education services. Further, Plaintiff J.B. provided PII based on the reasonable assumption that PowerSchool would provide prompt and timely notification of any unauthorized disclosure of PII to mitigate, among other things, the risks of identity theft and fraud. As a result of PowerSchool's misconduct, which caused the Data Breach, Plaintiff J.B. has, and will have to, take measures that would not otherwise be necessary to protect against identity theft and/or credit disruptions.

20. Plaintiff M.B. ("Plaintiff M.B.") is a minor resident and citizen of the State of New York and a student of Lynbrook North Middle School, an institution that relied on Defendant PowerSchool to manage the PII of its students and teachers. Plaintiff M.B. used PowerSchool products for education services, and provided highly sensitive PII to PowerSchool in order to receive education services. Plaintiff M.B. provided highly sensitive PII based on the reasonable assumption that PowerSchool would secure and safeguard PII with adequate security and privacy measures and protect PII from unauthorized disclosure and as a condition of receiving education services. Further, Plaintiff M.B. provided PII based on the reasonable assumption that PowerSchool would provide prompt and timely notification of any unauthorized disclosure of PII to mitigate, among other things, the risks of identity theft and fraud. As a result of PowerSchool's misconduct, which caused the Data Breach, Plaintiff M.B. has, and will have to, take measures that would not otherwise be necessary to protect against identity theft and/or credit disruptions.

21. Defendant PowerSchool is a Delaware company founded in 1997 and is headquartered at 150 Parkshore Drive, Folsom, CA 95630. Defendant offers a wide range of

products and services including: a Student Information System platform; document management system; enrollment/attendance manager; recruitment platform; parent communication platform; and Naviance, a tool for planning a student's academic success, to clients in the education industry. In 2024, PowerSchool was acquired by Bain Capital.

JURISDICTION & VENUE

22. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, and there are more than 100 putative Class Members, and at least one Class Member is a citizen of a state different from Defendant's to establish minimal diversity.

23. This Court has personal jurisdiction over Defendant PowerSchool in this action because PowerSchool conducts its substantial business in this District, and the conduct giving rise to this action arises out of and relates to those business dealings. Specifically, PowerSchool collects and maintains data of an estimated fifty (50) million students, including those located in this District.

24. PowerSchool derives substantial revenue from its contracts with schools and school districts in all fifty (50) states. Through the contracts it signs with educational institutions, PowerSchool collects, stores, and manages the highly sensitive PII and sensitive student records for millions of students and teachers across the United States.

25. Venue is proper in this District under 28 U.S.C. §1391(b) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

I. DEFENDANT ROUTINELY COLLECTS HIGHLY SENSITIVE PII FROM MILLIONS OF STUDENTS, TEACHERS, AND THEIR FAMILIES

26. Defendant PowerSchool is the largest provider of cloud-based education software for K-12 education in the United States, with 18,000 customers across North America, making it responsible for the PII of over fifty (50) million students, teachers, and their family members in the country. PowerSchool retains historical information of former students and teachers who previously made use of its systems, dating back to 2005.[6]

27. PowerSchool services its customers in more than ninety (90) countries including throughout North America—specifically, private and public schools and school districts. PowerSchool offers its school-customers a variety of products aimed at managing educational administrative tasks like enrollment, attendance, parent notifications, emergency contacts, assignments, grades, transcripts, student medical records, and staff recruitment.

28. PowerSchool also offers a variety of cloud-software products for schools to customize to meet their needs and accomplish administrative tasks. One of PowerSchool's leading products is the PowerSchool SIS, used by at least 15,000 schools and districts across the country.[7]

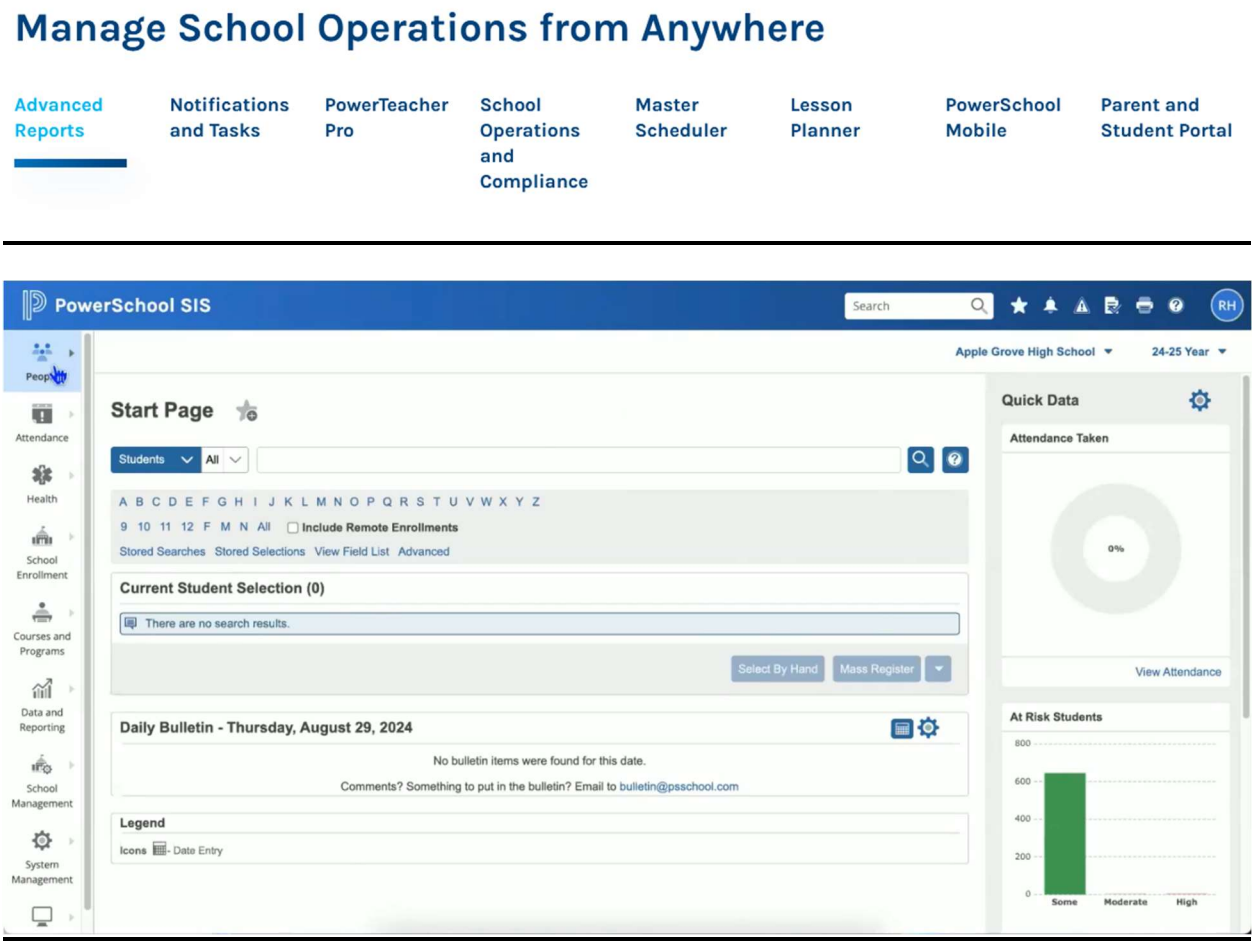
29. PowerSchool SIS is a comprehensive system designed to enable schools and school districts to collect and manage information related to the student body and teaching staff, including highly sensitive PII and sensitive student records. It includes configurable tools to help

---

[6] *PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data,* TechCrunch (Jan. 15, 2025 9:45PM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/.

[7] *40,000 Students Start School on Time Because of 90-Day PowerSchool SIS Implementation*, PowerSchool, https://www.powerschool.com/case-studies/40000-students-start-school-on-time-because-of-90-day-powerschool-sis-implementation/ (last visited Jan. 17, 2025).

create a portal for both students and parents to view academic performance and scheduling information; provides a communication platform for use by students, parents, teachers, and administrators; establishes a system to manage grades, attendance, assignments, and data entry; provides tools to monitor attendance, behavior, demographic, graduation tracking, and health related information; establishes a master scheduler for the institution; and facilitates the creation of lesson planners.



30. When its school-customers purchase and implement PowerSchool SIS, they gain access to customer support staff, training on how to use the system, and cybersecurity assistance.

31. As a condition of attending or working in PowerSchool's school-customers, students, teachers, staff, including their families, are required to utilize PowerSchool cloud

services. This means that students, teachers, staff, including their families, must enter their highly sensitive PII into PowerSchool systems as a condition of receiving education or maintaining their employment.

32. Indeed, as part of its services, PowerSchool collects and retains a wide variety of highly sensitive PII, including:[8]

- Name;
- Email Address;
- Social Security Number;
- Address;
- Phone Number;
- Emergency Contact Information;
- Birth Date;
- Age;
- Grade;
- Gender;
- Device Information (e.g. unique device ID, IP address, and cookies);
- Class Schedule;
- Standardized Test Scores;
- Grades;
- Allergy Information
- Immunization Records
- Learning Disabilities

[8] *PowerSchool's Privacy Principles*, PowerSchool, https://www.powerschool.com/privacy/ (last visited Jan. 17, 2025).

- Lunch Balances/Reduced Price Meal Status; and
- Attendance.

33. In order to provide its services, PowerSchool collects, stores, and maintains scores of data from its customers. PowerSchool's Global Privacy Statement states:[9]

> Depending on the PowerSchool Product(s) and/or Websites you utilize, we may collect personal information through the following means:
>
> - Directly from you (e.g., upon creating an account)
> - Automated data collection technologies (e.g., cookies, pixels)
> - Other sources (e.g., data analytics providers)

34. At base, this PII is highly sensitive and can be exploited by unauthorized parties to engage in fraudulent activities such as identity theft and other forms of fraud.

35. Moreover, this highly sensitive PII is legally protected by the Family Educational Rights and Privacy Act (FERPA)—a federal law aimed at protecting sensitive student records from being disclosed without the student's consent or knowledge.

36. Because of FERPA and other laws requiring the protection of PII, PowerSchool had a duty to adopt reasonable measures to protect the PII PowerSchool collected, which included confidential student records of Plaintiffs and Class Members from unauthorized access or disclosure to third parties.[10]

37. PowerSchool was also obligated to take steps to fulfill the representations PowerSchool made to the public about its ability to secure and safeguard PII, as discussed herein.

---

[9] *Id.*

[10] PowerSchool assumed a duty to Plaintiffs and Class Members as a third-party vendor relied upon by the educational institutions Plaintiffs and Class Members attended or were employed by.

II. DEFENDANT TOUTED THE SAFEGUARDS IT PUT IN PLACE TO PROTECT USER PII

38. Defendant PowerSchool knew or was negligent in not knowing of its duty to protect its customers' and users' highly sensitive PII and highly sensitive student records from unauthorized disclosure.

39. Legally, PowerSchool's duty arises from FERPA, other state and federal laws, common law, industry standards, and PowerSchool's own public representations concerning cybersecurity and privacy.

40. Separate and apart from PowerSchool's legal duty to its customers and users, PowerSchool made clear and explicit public representations to assure its customers and users that they could trust PowerSchool to safeguard the highly sensitive PII and educational records that PowerSchool collects.

41. PowerSchool admits its knowledge of its legal duties and responsibility to safeguard data on its public-facing website stating, "the safe collection and management of student data is essential to student success in the digital classroom."[11] PowerSchool further claims that it "knows the importance of understanding state-specific regulations, solving students' and educators' unique challenges, and supporting the needs of the local community."[12]

42. PowerSchool repeatedly made assurances to its customers, users, and the public that its collected data would be protected. PowerSchool's statements were as follows:

(a) "PowerSchool has signed the national Student Privacy Pledge regarding the collection, maintenance, and use of student personal information. The pledge states: 'School

[11] *Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited Jan. 17, 2025).

[12] *Personal Education for Every Journey*, PowerSchool, https://www.powerschool.com/ (last visited Jan. 17, 2025).

service providers take responsibility to both support the effective use of student information and safeguard student privacy and information security.'"[13]

(b) "PowerSchool certifies the application database, and infrastructure security of our software solutions."[14]

(c) "PowerSchool employs a variety of physical, administrative, and technological safeguards designed to protect your data against loss, misuse, and unauthorized access or disclosure. ***We strive to continuously maintain reasonable physical, administrative, and technical security measures.*** Our security measures consider the type and sensitivity of the data being collected, used, and stored, and the current state of technology and threats to data. Defendant independently verifies its security management system to the internationally recognized standard for security management and holds ISO 27001 and SOC2 certifications.

[13] *Student Data Privacy: Everything you Need to Know*, PowerSchool, https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/ (last visited Jan. 17, 2025).

[14] *Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited Jan. 17, 2025).

Defendant also endeavors to align its privacy and security operations to best practices and relevant international regulations."[15]

(d) "PowerSchool is committed to being a good custodian of student data – taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability. The company believes that the safe collection and management of student data is essential to student success within the 21st Century digital classroom."[16]

(e) "[T]he PowerSchool Information Security Report was born out of the K-12 Education Technology Secure by Design Pledge . . . The report is meant to provide our customers with additional transparency about cybersecurity at PowerSchool."[17]

PowerSchool Signs CISA's K-12 Education Technology Secure by Design Pledge

The quarterly issue of the PowerSchool Information Security Report was born out of the K-12 Education Technology Secure by Design Pledge. PowerSchool publicly agreed to the pledge at the White House ceremony in September 2023. The report is meant to provide our customers with additional transparency about cybersecurity at PowerSchool. It features cybersecurity trends in education as well as ways organizations can protect themselves.

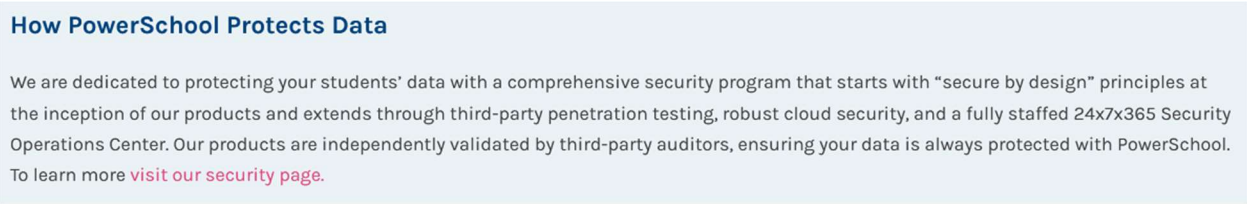
(f) "We are dedicated to protecting your students' data with a comprehensive security program that starts with 'secure by design' principles at the inception of our products

[15] *Privacy,* PowerSchool (last updated Feb. 2, 2023) https://www.powerschool.com/legal/privacy-2023/.

[16] *Student Data Privacy: Everything you Need to Know*, PowerSchool (June 20, 2023) https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/ .

[17] *Cybersecurity, Data Privacy, & Infrastructure,* PowerSchool, https://www.powerschool.com/security/ (last visited Jan. 17, 2025).

and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center. Our products are independently validated by third-party auditors, ensuring your data is always protected with PowerSchool."[18]


How PowerSchool Protects Data

We are dedicated to protecting your students' data with a comprehensive security program that starts with "secure by design" principles at the inception of our products and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center. Our products are independently validated by third-party auditors, ensuring your data is always protected with PowerSchool. To learn more visit our security page.

(g) "PowerSchool's commitment to being the most trusted edtech leader in student privacy protection and cybersecurity extends to our AI applications. We ensure that security best practices are incorporated during research and development as well as protecting our applications and customer data."[19]

(h) "We're dedicated to best-in-class security in our interoperable products, ass a company, and with our employees . . . we have the right security professionals, we have scale, and we want to take the discipline of data security even further."[20]

43. PowerSchool further represented that it was in compliance with applicable regulations, including FERPA, the General Data Protection Regulation (GDPR), the Children's Online Privacy Protection Act (COPPA), and other state and federal regulations, providing Plaintiffs and Class Members with additional assurances their data would be properly safeguarded.[21]

---

[18] *PowerSchool SIS*, PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last visited Jan. 17, 2025).

[19] *Responsible AI with Security by Design*, PowerSchool (Nov. 28, 2023) https://www.powerschool.com/blog/bring-ai-to-data/.

[20] *5 Ways Tech Directors Can Improve Student Data Security and Privacy Through Interoperability*, PowerSchool (Aug. 26, 2022) https://www.powerschool.com/blog/ways-tech-directors-can-improve-student-data-security-privacy-through-interoperability/.

[21] *See Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited Jan. 17, 2025).

44. By making these statements, and touting the security of its platforms, PowerSchool made repeated misrepresentations about the safety and security of the collected highly sensitive PII and educational records in PowerSchool's systems. PowerSchool was negligent and/or reckless in making these misstatements while operating systems subject to significant cybersecurity vulnerabilities, discussed further herein.

45. Despite experiencing the massive Data Breach in December 2024, PowerSchool ***continues*** to misrepresent the sufficiency of its products' security and privacy. As of January 17, 2025, PowerSchool's website continues to tout itself as a "good custodian of student data, taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability."[22] Several examples of PowerSchool's ***current public-facing representations*** regarding the security of its products are reproduced below:

(a) "PowerSchool certifies its software solutions' application, database, and infrastructure security."[23]

(b) "Parents can rest assured that PowerSchool is a trusted, verified custodian of their children's data."[24]

[22] *Id.*

[23] *Student Data Privacy: Everything You Need to Know,* PowerSchool (June 20, 2023), https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/ .

[24] *Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited Jan. 17, 2025).

Our Pledge of Student Privacy

PowerSchool has signed the national Student Privacy Pledge regarding the collection, maintenance, and use of student personal information. The pledge states: "School service providers take responsibility to both support the effective use of student information and safeguard student privacy and information security."

Assure Stakeholders That Your Student Data Is Safe

Schools and districts can communicate with confidence to shareholders that their student data is safe and secure.PowerSchool compliance initiatives are driven by many regulations, including:

- Family Educational Rights and Privacy Act Regulations (FERPA)
- General Data Protection Regulation (GDPR)
- Children's Online Privacy Protection Act
- Breach Laws, Data Residency Laws
- Digital Millenium Copyright Act (DMCA)
- Sarbanes-Oxley Act
- Sate contracts for reporting

Give Parents Peace of Mind

Parents can rest assured that PowerSchool is a trusted, verified custodian of their children's data. When a district or school partners with PowerSchool, parents and students are invited into the secure system and enter their information, with their consent.

(c) "We are dedicated to protecting your students' data with a comprehensive security program that states with 'secure by design' principles at the inception of our products and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center. Our products are independently validated by third-party auditors, ensuring your data is always protected with PowerSchool."[25]

How PowerSchool Protects Data

We are dedicated to protecting your students' data with a comprehensive security program that starts with "secure by design" principles at the inception of our products and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center. Our products are independently validated by third-party auditors, ensuring your data is always protected with PowerSchool. To learn more visit our security page.

46. For the reasons stated herein, Plaintiffs and Class Members entrusted PowerSchool with their highly sensitive PII and educational records as a condition of education and/or employment services based on, amongst other things, PowerSchool's representations about the sufficiency of its data management and security systems.

[25] *PowerSchool SIS,* PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last visited Jan. 17, 2025).

III. CONTRARY TO DEFENDANT'S REPRESENTATIONS, DEFENDANT FAILED TO REASONABLY SAFEGUARD USER PII

47. To date, Defendant PowerSchool has failed to provide all of the individuals affected by the Data Breach (students, teachers, staff, and their families) with a notice of data breach or data breach letter.

48. PowerSchool's letter correspondence related to this serious Data Breach has been ***limited to a customer letter addressed only to organizations*** containing limited information about affected individuals. A copy of the letter is attached hereto as **Exhibit A**.

49. On or about January 7, 2025, PowerSchool sent its school-customers a *Notice of Data Breach* (the "Notice").[26]

50. The Notice provided the following information:

> [W]e are reaching out to inform you that on December 28, 2024, PowerSchool become aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed.
>
> * * *
>
> As soon as we learned of the potential incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We have also informed law enforcement.
>
> We can confirm that the information accessed belongs to certain SIS customers and relates to families and educators, including those from your organization.[27]

[26] *PowerSchool*, https://www.powerschool.com/security/sis-incident/ (last visited Jan. 17, 2025).

[27] *See* Exhibit A.

51. PowerSchool provided this Notice to schools ***almost two (2) weeks after*** PowerSchool claims to have identified the Data Breach. By PowerSchool's own admission, the breach was identified on or about December 28, 2024, previous to which an unauthorized party gained access to, viewed, and downloaded Plaintiffs' and Class Members' PII and educational records from PowerSchool's network.

52. To date, PowerSchool has failed to provide sufficient notice of the Data Breach and the details surrounding the breach. PowerSchool's delay in notifying Plaintiffs and Class Members of the Data Breach likely violates the immediate notice requirement of N.Y. Gen. Bus. Law § 899-aa, and renders PowerSchool's security and privacy assurances material misrepresentations in violation of N.Y. Gen. Bus. Law §§349, 350.

53. PowerSchool has not, as of this date, offered any explanation for the delay in providing Plaintiffs and Class Members with notice of the Data Breach.

54. PowerSchool has not publicly identified the extent to which the Data Breach impacted its systems. Instead, it directs users to "reach out to your school directly" to determine if their PII or the PII of their children has been impacted.[28] PowerSchool has yet to provide any information regarding the extent of the fifty (50) million student records it holds were impacted, and provide no timeline for when PowerSchool plans to provide notice to Plaintiffs and Class Members.[29] PowerSchool's investigation regarding the Data Breach is ongoing and is likely to reveal the existence of additional impacted individuals and data.[30]

[28] *Id.*
[29] *Id.*
[30] *Id.*

55. The size and scope of the Data Breach is undoubtedly vast. Indeed, media outlets are referring to this Data Breach as "close to being the worst-case scenario."[31]

56. In fact, an independent investigation shows the breach also impacted former customers of PowerSchool, and that the number of affected students in certain school districts are four (4) to ten (10) times higher than the number of actively enrolled students in those districts.[32]

57. The scope of the Data Breach will only be made worse by PowerSchool's ongoing investigation and will likely reveal discovery of additional affected data and individuals.

58. Because PowerSchool's investigation is still ongoing, Plaintiffs and Class Members have no way of knowing the full impact of the Data Breach and the extent to which their highly sensitive PII has been misused.

59. According to the *Notice of Data Breach*, "an unauthorized party gained access" to PowerSchool's system through the use of "a compromised credential."

60. Compromised credentials are when an unauthorized user gains access to an authorized user's valid login information. This can occur when users re-use the same passwords across multiple websites, do not change their password frequently, or rely on overly simplistic passwords.

61. Such lax security practices allow hackers to use previously stolen credentials available on the black market or widely available password cracking tools, which use a variety of methods to guess passwords, to gain access to systems.

---

[31] Loraine Langreo, *Close to a 'Worst-Case Scenario': Cybersecurity Expert Discusses PowerSchool's Data Breach*, EDUCATION WEEK (Jan. 14, 2025), https://www.edweek.org/technology/close-to-a-worst-case-scenario-cybersecurity-expert-discusses-powerschools-data-breach/2025/01 .

[32] PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data, *TechCrunch* (Jan. 15, 2025 9:45PM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/ .

62. Entities and individuals can protect themselves from the use of compromised credentials through the use of MFA, which is a method of authenticating a user that does not rely solely on the use of a username and password.

63. MFA requires authorized users to input an additional piece of information that is requested at the time of login. This information can be, among other things, a randomly generated PIN number, biometric verification, or a physical token the authorized user possesses which verifies their identity.

64. The use of MFA is widely recognized as a critical element of digital security. Passwords can be easily acquired on the black market, but the additional protection provided by MFA can maintain account security despite compromised credentials. Its use is recommended by both the National Institute of Standards and Technology ("NIST") and Microsoft due to its effectiveness and the inability of passwords alone to effectively secure a system.[33]

65. PowerSchool did not use MFA to secure its systems or relied on improperly configured MFA, despite its use being widely acknowledged as best-practice.[34]

66. To mitigate the impact of potential data breaches, it is also industry best practice to delete PII once it is no longer necessary for an organization's business purpose. According to NIST, "[i]f PII is no longer relevant and necessary, then PII should be properly destroyed."[35]

---

[33] *Multi-Factor Authentication*, NIST (last updated March 12, 2024) https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication ; *What is: Multifactor Authentication*, Microsoft, https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661 (last visited Jan. 17, 2025).

[34] *PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data,* TechCrunch (Jan. 15, 2025 9:45PM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/ .

[35] *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* NIST (Apr. 2010), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf .

67. By disposing of information that is no longer necessary for the operations of the business, entities can reduce the impact of a data breach.

68. PowerSchool retained data of its users, even after users were no longer attending or employed by the school-customer, dating back to the start of the 2009-2010 school year.[36]

69. On information and belief, the highly sensitive PII and educational records PowerSchool failed to safeguard were unencrypted, which has made or will make it easier for cybercriminals and hackers to misuse Plaintiffs' and Class Members' data. Such data has already been accessed and viewed by unauthorized third parties.

70. Despite PowerSchool's failure to notify impacted individuals about the Data Breach, PowerSchool claims that they "take [their] responsibility to protect student, family, and educator data privacy extremely seriously, and [] are committed to providing customers, families, and educators with resources and support as we work through this together."[37] However, Defendant has failed to provide sufficient details about the cause of the Data Breach, the vulnerabilities hackers and/or cybercriminals exploited, the unauthorized third party or parties that initiated the cyber-attack, and the remedial measures undertaken to ensure a breach does not occur again.

71. The *Notice of Data Breach* provided by PowerSchool is inadequate. Not only has such notice never been provided to Plaintiffs and Class Members, but Defendant also failed to provide specific details about the breach that are necessary for Plaintiffs and Class Members to mitigate the imminent risk of identity theft and fraud. Specifically, Defendant has failed to: (i) disclose what parties or individuals have been impacted by the breach; (ii) disclose or identify

[36] *PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data*, TechCrunch (Jan. 15, 2025 9:45PM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/ .

[37] *PowerSchool*, https://www.powerschool.com/security/sis-incident/ (last visited Jan. 17, 2025).

the unauthorized third party; (iii) disclose the network or system vulnerabilities that allowed the unauthorized third party to gain access to Plaintiffs' and Class Members' PII, including confidential student records; and (iv) specify the scope of the Data Breach, including the time period during which the compromised data was accessed or collected.

72. Plaintiffs' and Class Members' data has been compromised and is likely to be misused by: (i) being put up for sale on the dark web; (ii) being exploited by criminals for illegal purposes; or (iii) being used for targeted marketing without Plaintiffs' and Class Members' knowledge or consent.

73. This information and the full scope of the Data Breach —which is not yet known —is critical to Plaintiffs and Class Members, in part, because PowerSchool continues to maintain possession, custody, and control over Plaintiffs' and Class Members' data. Plaintiffs and Class Members have no way of knowing whether PowerSchool has completely resolved the Data Breach and whether PowerSchool has taken the steps necessary to prevent continued or repeated unauthorized access to its users' highly sensitive PII and educational records going forward. Thus, Plaintiffs' and Class Members' data remain at risk on PowerSchool's systems as well as at a risk of sale or exposure to fraudulent actors.

IV. COMPROMISED DATA IS HIGHLY VALUABLE TO HACKERS AND CYBERCRIMINALS

74. Cyberattacks by hackers and cybercriminals are pervasive and rapidly increasing in frequency. In a recent report, Forbes stated that the number of data breaches exceeded 1,571 in the first half of 2024, a 14% increase compared to the same period in 2023.[38]

[38] *Why Data Breaches Are Increasing And What CISOs Can Do About It,* Forbes (Jan. 14, 2025 9:03 a.m.), https://www.forbes.com/sites/forbestechcouncil/2023/04/20/why-data-breaches-are-increasing-and-what-cisos-can-do-about-it/?sh=7e83992c547e .

75. Educational institutions and its associated vendors are acutely aware that their databases are a central target of cybercriminals due to their storage of vast amounts of PII, including confidential student records. Data breaches of education-related organizations are occurring with increased frequency because educational institutions collect sensitive PII.[39] A 2022 report published by the United States Government Accountability Office states that:

> according to data from the MS-ISAC, reported ransomware incidents against K-12 schools increased significantly in August and September 2020. ***Fifty-seven percent of all ransomware incidents reported to the MS-ISAC involved K-12 schools***, compared to 28 percent of reported ransomware incidents around the end of the 2019-2020 school year (January through July 2020).[40]

76. Education-related PII is highly valuable to hackers. Recent studies show that hackers value PII over other categories of data, such as credit card information and passwords. Accordingly, "PII is the most valuable since criminals can compile more PII from the dark web to then engage in harder to prevent fraud or full-on identity theft."[41]

77. Hackers and cybercriminals seek to amass PII because individual data points can "be pieced together like a puzzle" to "complete an online profile of" a person and "impersonate you or others online."[42] In addition to seeking PII for identity theft, hackers seek PII to sell and profit from on the dark web.

78. Experian describes the dark web as "a huge marketplace for stolen data and personal information. After a data breach or hacking incident, personal information is often

---

[39] *One Reason School Cyberattacks Are On the Rise? Schools Are Easy Targets for Hackers,* NPR (Mar. 11, 2024 3:00 p.m.), https://www.npr.org/2024/03/11/1236995412/cybersecurity-hackers-schools-ransomware .

[40] *Critical Infrastructure Protection: Additional Federal Coordination is Needed to Enhance K-12 Cybersecurity,* U.S. Government Accountability Office (Oct. 20, 2022), https://www.gao.gov/products/gao-23-105480.

[41] *Hackers Went After Personally Identifiable Information the Most, Study Says,* SC Media (Jan. 5, 2023), https://www.scmagazine.com/news/hackers-went-after-personally-identifiable-information-the-most-study-says .

[42] *What is PII and Why Criminals Want Yours,* Cyber Defense Magazine (Feb. 28, 2019), https://www.cyberdefensemagazine.com/what-is-pii-and-why-criminals-want-yours/ .

bought and sold on the dark web."[43] For this reason, Plaintiffs and Class Members face an imminent risk of having their PII—which was accessed, viewed, and downloaded in connection with this Data Breach—sold on the dark web.

79. Consumer data is highly valuable on the dark web. According to CyberDefense Magazine, "[o]n average, a consumer's passwords sell for around $80, while even small details like purchase history can sell for $20. Credit card numbers can sell for as little $5, while passports might fetch up to $2,000."[44]

80. A Dark Web Price Index study conducted by Privacy Affairs found that a "full range of documents and account information that will allow identity theft" can be bought for approximately $1,000."[45]

81. Student records are particularly valuable to identity thieves and other criminals, because such records provide a complete profile of an individual and that individual is more likely to have no previous credit history, making their PII particularly useful for financial scams.

82. The Department of Education has identified the value of a student record on the black market at $250-$300, a fact known to PowerSchool, as it uses this figure to promote its own products.[46]

---

[43] *Here's How Much Your Personal Information Is Selling for on the Dark Web,* Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ .

[44] Cyber Defense Magazine, *supra* note 40.

[45] *Revealed – How Much is Personal Information Worth on the Dark Web?* Insurance Business (May 1, 2023) https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx .

[46] *Student Data Privacy: Everything You Need to Know*, PowerSchool (Jun. 20, 2023), https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/ .

83. PowerSchool is well aware of the cyber risks that educational organizations face. The risks are especially well-known because PowerSchool has previously experienced other data breaches and cyber-attacks.[47]

V. DEFENDANT FAILED TO EMPLOY REASONABLE SAFEGUARDS FOR PLAINTIFFS' AND CLASS MEMBERS' PII

84. Defendant PowerSchool failed to employ reasonable safeguards, pursuant to regulatory guidelines and widely-recognized industry standards commensurate with the highly sensitive nature of the PII at issue. As a result of PowerSchool's negligence, Plaintiffs' and Class Members' highly sensitive PII was accessed, viewed, and downloaded by unauthorized third parties in the Data Breach. PowerSchool flouted scores of guidelines set forth by government agencies and industry experts and failed to implement them.

A. Regulatory Requirements and Guidelines

85. The Federal Trade Commission ("FTC") has set forth specific guidelines about reasonable safeguards for data. The FTC's "*Start with Security: A Guide for Business*" paper instructs companies to "know what personal information you have in your files and on your computers, and keep only what you need for your business . . . protect the information that you keep, and properly dispose of what you no longer need," and "create a plan to respond to security incidents."[48]

---

[47] *Cybersecurity, Data Privacy, & Infrastructure,* PowerSchool, https://www.powerschool.com/security/ (last visited Jan. 17, 2025).

[48] Fed. Trade Comm'n, *Start with Security: A Guide for Business (*Aug. 2023*)*, https://www.ftc.gov/business-guidance/resources/start-security-guide-business .

86. The FTC also instructs business to "take reasonable steps" to keep personal data secure.[49] This includes "put[ting] controls in place to make sure employees have access only on a 'need to know' basis."[50] The FTC also recommends using "separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases."[51] Moreover, "[i]f employees don't have to use personal information as part of their job, there's no need for them to have access to it."[52]

87. Importantly, the FTC advises companies to "store sensitive personal information securely" especially during transmission.[53] The FTC recommends that companies "use strong cryptography to secure confidential material during storage and transmission." This includes "mak[ing] sure the people you designate to do that job understand how your company uses sensitive data and have the know-how to determine what's appropriate for each situation."[54]

88. The New York State Department of Financial Services ("NYSDFS") has also issued guidelines for cybersecurity, including a checklist exhibiting data security best practices. One such best practice is to "review and manage user access privileges" on an annual basis to ensure that such user access privileges are sufficiently limited to avoid vast access points to entities' systems.[55]

89. The NYSDFS recommends that entities' annual access review include ensuring that "users are required to authenticate themselves" and implementing controls like multi-factor

---

[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Part 500 Requirements Checklist for DFS,* NYDFS https://www.dfs.ny.gov/system/files/documents/2024/08/Cyber-WD-Part500-Requirement-Checklist.pdf (last accessed Jan. 17, 2025).

authentication to maintain secure remote connections and avoid creating data access points for third parties.[56]

90. PowerSchool did not adequately comply with these guidelines as evidenced by its *Notice of Data Breach*, which confirmed that a single compromised credential allowed the hackers to access data of an undisclosed number of students and teachers from at least 77 different school districts in the United States[57]. This misconduct is indicative of PowerSchool's failure to take reasonable steps to protect Plaintiffs' and Class Members' PII, as allowing unauthorized account access to so much PII does not conform to the best practices recommended by the FTC.

B. Industry Standards

91. The National Institute of Standards and Technology ("NIST"), provides guidance designed to "[help] businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data."[58] According to NIST, "Passwords alone are not effective in securing your most sensitive business assets, as they have become too easy for threat actors to access. [MFA] is an important security enhancement that requires a user to verify their identity by providing more than just a username and password."[59]

[56] Cybersecurity Template, NYDFS (May 2024) https://www.dfs.ny.gov/system/files/documents/2024/05/Cybersecurity-Program-Template_05.2024.pdf .

[57] *PowerSchool hack exposes student, teacher, data from K-12 districts*, Bleeping Computer (Jan. 7, 2025), https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/ .

[58] *Understanding the NIST Cybersecurity Framework*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last visited Jan. 17, 2025).

[59] *Multi-Factor Authentication*, NIST https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication (last visited Jan. 17, 2015).

92. PowerSchool did not implement reasonable or proper protocols for authorization and access to their networks and systems, including MFA, which contributed to the Data Breach.[60]

93. The NIST Cybersecurity Framework recommends that "organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the purpose."[61]

94. PowerSchool retained PII of its users long after such information was no longer relevant for a legitimate business purpose, including after individuals were no longer attending or employed by the school-customers, dating back to the start of the 2009-2010 school year.[62]

95. PowerSchool failed to follow the reasonable guidelines and other industry best practices put forth by the FTC, NYDFS, and NIST, and, as a result, failed to safeguard Plaintiffs' and Class Members' highly sensitive PII and educational records from unauthorized disclosure.

96. PowerSchool could have prevented the Data Breach by implementing the security and privacy measures recommended by federal and state government agencies and industry organizations. Such measures would have involved proper encryption of Plaintiffs' and Class Members' PII and the proper implementation of MFA. Moreover, PowerSchool should have destroyed the data that was no longer relevant or needed.

---

[60] *PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data*, TechCrunch (Jan. 15, 2025 9:45PM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/ .

[61] *SA-8 (33): Minimization*, CSF Tools, https://csf.tools/reference/nist-sp-800-53/r5/sa/sa-8/sa-8-33/ (last visited Jan. 17, 2025).

[62] *PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data*, TechCrunch (Jan. 15, 2025 9:45PM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/ .

97. PowerSchool's failure to safeguard the data of Plaintiffs and Class Members is made worse by the fact that PowerSchool was repeatedly made aware of the foreseeable cybersecurity and privacy risks to educational organizations. Despite these clear warnings, PowerSchool failed to secure and safeguard Plaintiffs' and Class Members' data.

98. PowerSchool's failure to protect Plaintiffs' and Class Members' PII from unauthorized disclosure is made even worse by the fact that Defendant admittedly appreciated the grave dangers of identity theft associated with PII. Specifically, Defendant told the public that, "From 2018 to 2022, 2 million students have been affected by ransomware attacks, and in 2022 alone, data was exfiltrated in at least 58 school incidents. Globally, 56% of K-12 schools experienced a cyberattack."[63] In making this public disclosure, PowerSchool assured the public that it was aware of cyber risks. Taken with PowerSchool's public representations about cybersecurity and privacy, these public disclosures assured Plaintiffs and Class Members that they could trust PowerSchool with their PII.

VI. THIS DATA BREACH WILL RESULT IN ADDITIONAL IDENTITY THEFT AND FRAUD

99. Because of the Data Breach—caused by Defendant's misconduct—Plaintiffs and Class Members face an increased (and imminent) risk of identity theft or fraud. In fact, unbeknownst to Plaintiffs and Class Members, they may have already suffered from identity theft or fraud in connection with the Data Breach. Additionally, breaches, like PowerSchool's Data Breach, cause significant disruption to impacted individuals' daily lives.

100. Plaintiffs and Class Members face several types of identity theft and fraud including financial identity theft, medical identity theft, criminal identity theft, synthetic identity

[63] *4 Reasons Why a Robust K-12 SIS is a Smart Long-Term Investment*, PowerSchool (June 2, 2023) https://www.powerschool.com/blog/4-reasons-why-a-robust-sis-is-a-smart-long-term-investment/ .

theft, and child identity theft. These forms of identity theft can result in credit card fraud, fraud through government documents and benefits, bank fraud, employment fraud, tax fraud, and medical fraud.[64]

101. The risk of identity theft to data breach victims is pervasive and continues for years after a data breach. According to a 2017 Javelin strategy and research presentation, fraud based on data that is two (2) to six (6) years old has increased by nearly 400%.[65]

102. Children are equally (and especially) at risk of identity theft when their highly sensitive PII is compromised. Indeed, credit reporting agencies do not routinely check applicants' age or adequate proof of identity—meaning the agencies will not serve as a sufficient defense against the illicit use of children's name, date of birth, or SSN.[66]

103. Any relief PowerSchool purports to provide will not be sufficient in protecting Plaintiffs and Class Members from the imminent risks of potential identity theft or fraud that they will face for years to come. In fact, any potential attempt by PowerSchool to remedy the situation may be too late given PowerSchool's failure to notify impacted individuals thus far.

VII. PLAINTIFFS AND CLASS MEMBERS SUFFERED DAMAGES

104. The Data Breach was a direct and proximate result of PowerSchool's failure to properly safeguard and protect Plaintiffs' and Class Members' data from unauthorized access, use, and disclosure, as required by FERPA, various other state and federal regulations, industry practices, and the common law, including PowerSchool's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and

[64] *A Guide to Identity Theft Statistics for 2025*, McAfee, https://www.mcafee.com/learn/a-guide-to-identity-theft-statistics/ (last visited Jan. 17, 2025).

[65] Experian, *supra* note 22.

[66] *The Looming Crisis of Child Identity Theft*, Security Intelligence (Dec. 2, 2014) https://securityintelligence.com/the-looming-crisis-of-child-identity-theft/ .

confidentiality of Plaintiffs' and Class Members' data to protect against reasonably foreseeable threats to the security or integrity of such information.

105. Plaintiffs' and Class Members' PII and educational records are private and sensitive in nature and PowerSchool failed to adequately safeguard this information.

106. PowerSchool did not obtain Plaintiffs' and Class Members' consent to disclose their data to any other person or entity as required by applicable law and industry standards.

107. As a direct and proximate result of PowerSchool's wrongful action and inaction and the resulting Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from the possibility of identity theft or identity fraud by hackers and cybercriminals requiring them to undertake additional measures to mitigate the actual and potential impact of the Data Breach on their lives that they would not otherwise have to undertake. Such measures include: (i) implementing credit freezes; (ii) setting alerts with credit reporting agencies; (iii) alerting financial institutions; (iv) alerting medical providers; (v) closing or modifying bank accounts; and (vi) monitoring credit reports for unauthorized activity.

108. PowerSchool's misconduct directly and proximately caused the Data Breach which subjected Plaintiffs' and Class Members' highly sensitive PII and educational records to unauthorized disclosure without their knowledge or consent. As a result of PowerSchool's misconduct, Plaintiffs and Class Members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including: (i) theft of their valuable PII, which includes highly sensitive medical information and student records; (ii) imminent injury from identity theft; (iii) inability to sufficiently mitigate the risks of identity

theft and fraud due to Defendant's untimely disclosures of the Data Breach; (iv) loss of privacy; (v) the payment of costs to remedy or mitigate the effects of the Data Breach.

109. Because PowerSchool has not completed its investigation of the Data Breach, Plaintiffs and Class Members face a continued, unknown risk of additional harm which will only be revealed upon PowerSchool's completion of the investigation.

110. Additionally, Plaintiffs and Class Members face an ongoing risk of harm because PowerSchool continue to maintain possession, custody, and control over Plaintiffs' and Class Members' PII and educational records.

111. While the data of Plaintiffs and Class Members has been accessed or stolen, a copy of the same data continues to be held by PowerSchool. Plaintiffs and Class Members have an undeniable interest in ensuring that their data is secure, remains secure, and is not subject to further breach or theft.

CLASS ALLEGATIONS

112. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

113. The Class that Plaintiffs seek to represent is categorized and defined as follows:

> All individuals identified by PowerSchool Holdings, Inc. whose personally identifiable information ("PII") was compromised, accessed, or disclosed in the breach that is the subject of the Notice of Data Breach that Defendant PowerSchool Holdings, Inc. distributed on or about January 7, 2025 (the "Class").

114. Excluded from the Class are the following individuals and/or entities: (i) any Judge or Magistrate presiding over this action, any members of their immediate families, and any of their staff; (ii) the Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, assigns, current and former employees, officers, and directors, and any entity in

which the Defendant has a controlling interest; and (iii) Plaintiffs' counsel and Defendant's counsel.

115. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

116. **Numerosity (Rule 23(a)(1))**: The exact number of members of the Class is unknown and currently unavailable to Plaintiffs, but joinder of individual members herein is impractical. The Class is likely comprised of thousands of individuals. Defendant retains the data of fifty (50) million students, each of whom could be a member of the Class, and each of whom may have a guardian or multiple guardians who could also be a member of the Class. Moreover, over seventy-seven (77) school districts across the United States have been identified as having been impacted by the breach.[67] The precise number of Class Members, including their addresses, are unknown to Plaintiffs at this time, but can be ascertained from PowerSchool's records. The Class Members may be notified of the pendency of this action by mail or email, internet postings and/or publications, and supplemented (if deemed necessary or appropriate by the Court) by published notice.

117. **Predominant Common Questions of Law and Fact (Rule 23(a)(2))**: The Class's claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. The common and legal questions include, without limitation:

(a) Whether Defendant had a duty to protect the PII of Plaintiffs and Class Members;

[67] Lawrence Abrams, *PowerSchool hack exposes student, teacher data from K-12 districts*, BLEEPING COMPUTER (Jan. 7, 2025), https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/ .

(b) Whether Defendant had a duty not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

(c) Whether Defendant failed to adequately secure and safeguard the PII of Plaintiffs and Class Members;

(d) Whether Defendant timely learned of the Data Breach;

(e) Whether Defendant made an untimely disclosure of the Data Breach to Plaintiffs and Class Members;

(f) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate for the nature and scope of the information compromised in the Data Breach;

(g) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to secure and safeguard the PII of Plaintiffs and Class Members;

(h) Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

(i) Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

(j) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm they face as a result of the Data Breach.

118. **Typicality of Claims (Rule 23(a)(3))**: Plaintiffs' claims are typical of the claims of the Class because Plaintiffs, like all other Class Members, had their PII compromised in the Data Breach, suffered damages as a result of that Data Breach, and seek the same relief as the Class Members.

119. **Adequacy of Representation (Rule 23(a)(4))**: Plaintiffs adequately represent the Class because their interests do not conflict with the interests of Class Members, and they have retained counsel competent and experienced in complex class actions and consumer litigation.

120. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class.

121. **Superiority (Rule 23(b)(3))**: A class action is superior to other available means of adjudication for this controversy. It would be impracticable for Class Members to individually litigate their own claims against Defendant because the damages suffered by Plaintiffs and the members of the Class are relatively small compared to the cost of individually litigating their claims. Individual litigation would create the potential for inconsistent judgments and delay and expenses to the court system. A class action provides an efficient means for adjudication with fewer management difficulties and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Class against Defendant)

122. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

123. Defendant required Plaintiffs and Class Members to entrust Defendant with Plaintiffs' and Class Members' PII as a condition of receiving education related services.

124. A special relationship exists between Defendant and Plaintiffs and Class Members because Defendant provided the SIS that Plaintiffs and Class Members utilized as part of their education.

125. Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in collecting, obtaining, retaining, storing, securing, safeguarding, sharing, deleting, and

protecting Plaintiffs' and Class Members' PII in Defendant's possession from being compromised, breached, lost, stolen, accessed, or misused by unauthorized persons or entities. Specifically, Defendant had a duty to: (i) reasonably implement, design, and maintain security and privacy measures or systems to secure and safeguard Plaintiffs' and Class Members' PII; (ii) adequately test Defendant's security and privacy measures or systems; (iii) vet and test the security and privacy measures or systems of vendors to ensure that Plaintiffs' and Class Members' PII was reasonably secured and safeguarded; (iv) implement measures to detect system vulnerabilities, breaches, unauthorized access, or cyber-attacks in a timely manner; (v) implement a reasonable protocol to respond to system vulnerabilities, breaches, unauthorized access, or cyber-attacks in a timely manner to mitigate risks to Plaintiffs' and Class Members' PII; (vi) timely notify partners, vendors, customers, users, and other related entities, regarding vulnerabilities, breaches, unauthorized access, or cyber-attacks to its networks; and (vii) maintain data security measures consistent with industry standards.

126. Defendant's duties arose from the common law and statutes cited herein. Under the law, Defendant had a duty to secure and safeguard Plaintiffs' and Class Members' PII, including confidential student records, and a duty to timely disclose any unauthorized access to or theft of PII to Plaintiffs and Class Members. Further, Defendant had a duty to prevent foreseeable harm to Plaintiffs and Class Members. Defendant was aware that the risk of unauthorized access, data breach, or cyber-attack was foreseeable. Defendant was also aware that the PII of Plaintiffs and Class Members was the foreseeable and probable target of unauthorized third parties, such as hackers or cybercriminals.

127. Defendant breached its duty to reasonably safeguard the PII of Plaintiffs and Class Members and its duty to timely notify Plaintiffs and Class Members of the Data Breach.

Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach, instead only providing notice to impacted institutions on or about January 7, 2025.

128. Additionally, Defendant has failed to provide sufficient information to Plaintiffs and Class Members about the Data Breach despite the fact that it has been at least two (2) weeks since the Data Breach was discovered. To date, Defendant has failed to: (i) disclose or identify the unauthorized third party or parties; (ii) disclose the network or system vulnerabilities that allowed the unauthorized third party to gain access to Plaintiffs' and Class Members' PII, including confidential student records; and (iii) specify the scope of the Data Breach, including the time period during which the compromised data was collected. Further, Defendant breached its duty owed to Plaintiffs and Class Members by failing to provide timely and sufficient notice of the Data Breach to Plaintiffs and Class Members.

129. Defendant breached its duty owed to Plaintiffs and Class Members by, among other things, failing to safeguard Plaintiffs' and Class Members' PII from disclosure to unauthorized third parties. Specifically, Defendant's breach resulted in unauthorized third parties accessing, viewing, downloading, or misusing Plaintiffs' and Class Members' PII.

130. Because of Defendant's untimely and inadequate notice, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII, including, but not limited to medical information and bank account information.

131. Defendant further breached its duty owed to Plaintiffs and Class Members by, upon information and belief, improperly, inadequately, and unreasonably storing the PII of Plaintiffs and Class Members in ways that deviate from governing laws and industry rules, regulations, and practices. As a result, Defendant failed to safeguard Plaintiffs' and Class Members' PII.

132. Defendant's failure to reasonably and properly safeguard Plaintiffs' and Class Members' PII constituted a breach of Defendant's duty to protect PII and prevent unauthorized disclosure or access to PII by third parties.

133. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' PII would not have been compromised, accessed, viewed, downloaded, misused, stolen, or illegally sold by an unauthorized third party or parties.

134. Moreover, Defendant's failure to comply with the applicable laws and regulations constitutes negligence *per se*.

135. Because of Defendant's failure to reasonably safeguard Plaintiffs' and Class Members' PII, Plaintiffs and Class Members have suffered and will continue to suffer injury and damages.

136. Since being made aware of Defendant's *Notice of Data Breach*, Plaintiffs and Class Members have taken and must continue to take affirmative steps to ensure that their identities and financial information are not stolen or misused. But for Defendant's breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have to take these affirmative steps.

137. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including: (i) theft of their PII, which includes highly sensitive medical information; (ii) imminent and future injury from identity theft; (iii) inability to mitigate the risks of identity theft or fraud due to Defendant's untimely disclosures of the Data Breach; (iv) loss of privacy; (v) the payment of costs to remedy or

mitigate the effects of the Data Breach, including, but not limited to, payment for credit monitoring services.

138. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class against Defendant)

139. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

140. Defendant invited school-customers to implement its EdTech services. For this reason, Plaintiffs and Class Members used Defendant's products for educational services. Plaintiffs and Class Members accepted Defendant's education related services.

141. When Plaintiffs and Class Members sought and accepted education related services from institutions that contracted with Defendant, they were required to provide their PII to Defendant. Plaintiffs provided their PII to Defendant in order to receive education related services.

142. As set forth above, Plaintiffs and Class Members entrusted Defendant with their PII, in part, because Defendant repeatedly represented that it would secure and safeguard users' PII. Upon providing their PII to Defendant, Plaintiffs and Class Members entered into implied contracts with Defendant under which Defendant agreed to secure and safeguard Plaintiffs' and Class Members' PII and to timely and sufficiently notify Plaintiffs and Class Members of security vulnerabilities, data breaches or unauthorized disclosures.

143. All education related services sought by Plaintiffs and Class Members were sought pursuant to mutually agreed-upon implied contracts with Defendant under which

Defendant agreed to safeguard and protect Plaintiffs' and Class Members' PII and to provide timely and sufficient notice if such information was subject to security vulnerabilities, data breaches or unauthorized disclosures.

144. Without Defendant's representations that user PII would be safeguarded, Plaintiffs and Class Members would not have provided their PII to Defendant.

145. Further, without the existence of the implied contracts described herein, Plaintiffs and Class Members would not have provided their PII to Defendant.

146. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

147. Defendant breached the implied contracts it entered into with Plaintiffs and Class Members by failing to reasonably secure and safeguard Plaintiffs' and Class Members' PII. Further, Defendant breached the implied contracts it entered into with Plaintiffs and Class Members by failing to timely and sufficiently notify Plaintiffs and Class Members of the Data Breach which resulted in unauthorized disclosures of their PII.

148. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant and Plaintiffs and Class Members, Plaintiffs and Class Members were injured and continue to be injured, as set forth herein, and sustained actual losses and damages.

COUNT III
VIOLATIONS OF THE NEW YORK GENERAL BUSINESS LAW § 349, *et seq.*
(On behalf of Plaintiffs and the Class against Defendant)

149. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

150. New York General Business Law Section 349(a) ("Gen. Bus. Law § 349") declares unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state."

151. Plaintiffs and the Class Members are "person[s]" within the meaning of N.Y. Gen. Bus. Law § 349(h).

152. Defendant is a "person[s], firm[s], corporation[s] or association[s]" within the meaning of N.Y. Gen. Bus. Law § 349(b).

153. Defendant engaged in deceptive acts and practices in the conduct of its business, trade, and commerce, in violation of N.Y. Gen. Bus. Law § 349, including: (i) failing to develop, implement, and maintain reasonable security and privacy measures to protect the PII of Plaintiffs and Class Members from unauthorized disclosure; (ii) failing to implement sufficient risk management protocols to mitigate the foreseeable security or privacy risks to Plaintiffs' and Class Members' PII; (iii) failing to reasonably or sufficiently improve their security or privacy measures or systems to reasonably safeguard Plaintiffs' and Class Members' PII from unauthorized disclosure; (iv) failing to comply with legal duties requiring Defendant to reasonably secure and safeguard Plaintiffs' and Class Members' PII, which includes highly sensitive student records; (v) misleading Plaintiffs and Class Members to believe that Defendant would secure and safeguard Plaintiffs' and Class Members' PII by, among other things, misrepresenting the security or privacy measures or systems Defendant put in place; and (vi) failing to timely or sufficiently disclose the material fact that, because of Defendant's misconduct, Plaintiffs' and Class Members' PII was compromised, subject to the Data Breach, and viewed, accessed, downloaded, misused, or stolen by third parties without Plaintiffs' and Class Members' knowledge or consent.

154. Defendant's deceptive acts and practices, including, but not limited to those stated herein, were a direct and proximate cause of the Data Breach.

155. Defendant's concealment of the true timing and scope of the Data Breach was material to Plaintiffs and Class Members.

156. The conduct alleged herein constitutes recurring, "unlawful" deceptive acts and practices in violation of Gen. Bus. Law § 349, and as such, Plaintiffs and Class Members seek monetary damages and the entry of preliminary and permanent injunctive relief against Defendant, requiring Defendant to implement reasonable and sufficient safeguards over user data to prevent further unauthorized disclosure.

157. Defendant made affirmative misrepresentations to Plaintiffs and Class Members that Defendant was securely collecting, maintaining, and safeguarding users' highly sensitive PII from unauthorized disclosure. Defendant, however, concealed, and suppressed material facts concerning their unreasonable security and privacy measures, their unauthorized disclosure of Plaintiffs' and Class Members' PII in the Data Breach, and the full scope of the Data Breach.

158. Defendant had an ongoing duty to Plaintiffs and Class Members to refrain from unfair and deceptive practices. Specifically, Defendant owed Plaintiffs and Class members a duty to disclose all the material facts regarding the unauthorized disclosure of their highly sensitive PII, including without limitation student records protected by FERPA.

159. Plaintiffs and Class Members had no way of discerning that Defendant's representations were false and misleading because Plaintiffs and Class Members did not have access to Defendant's internal technology, data storage, or privacy systems and software.

160. Defendant thus violated Gen. Bus. Law § 349 by making statements that, when considered from the perspective of the reasonable consumer, conveyed that users' highly sensitive PII was secure and safeguarded from unauthorized disclosure. Defendant intentionally and knowingly made affirmative misrepresentations and failed to disclose material facts

regarding the Defendant's failure to safeguard users' PII after discovering the Data Breach. Defendant knew or should have known that its conduct violated Gen. Bus. Law § 349.

161. Defendant owed Plaintiffs and Class Members a duty to safeguard their highly sensitive PII and alert them of any unauthorized disclosure in a timely manner with specificity.

162. Plaintiffs and Class Members suffered ascertainable losses and actual damages as a direct and proximate result of Defendant's misrepresentations and concealment of and failure to disclose material information. Defendant had an ongoing duty to all its customers and the public to refrain from unfair and deceptive practices. Plaintiffs and Class Members incurred or will continue to incur costs, including for, among other things, credit freezes, disruptions to credit scores and history, or identity theft protection services. Moreover, Plaintiffs and Class Members were injured by Defendant because, among other things, the Defendant's actions caused: (i) theft of Plaintiffs' and Class Members' PII, which includes highly sensitive medical information; (ii) imminent injury from identity theft; (iii) inability to mitigate the risks of identity theft and fraud due to Defendant's untimely disclosures of the Data Breach; (iv) loss of privacy; (v) the payment of costs to remedy or mitigate the effects of the Data Breach, including, but not limited to, payment for credit monitoring services.

163. Defendant's deceptive and unlawful practices affected the public interest and consumers generally, including hundreds (if not thousands) of New Yorkers affected by the Data Breach.

164. Defendant's deceptive and unlawful practices present a continuing risk to Plaintiffs and Class Members as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

165. Plaintiffs and Class Members seek monetary relief against Defendant measured as the greater of (i) actual damages in an amount to be determined at trial, and (ii) statutory damages for each Class member. Plaintiffs and Class Members also seek an order enjoining Defendant's deceptive acts and practices, attorneys' fees, and any other just and proper relief under N.Y. Gen. Bus. Law § 349.

COUNT IV
VIOLATIONS OF THE NEW YORK DECEPTIVE SALES PRACTICE ACT
New York Gen. Bus. Law § 350, *et seq.*
(On behalf of Plaintiffs and the Class against Defendant)

166. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

167. N.Y. Gen. Bus. Law § 350 provides, in part, that "[f]alse advertising in the conduct of any business, trade or commerce or in the furnishing of any service in this state is hereby declared unlawful."

168. N.Y. Gen. Bus. Law § 350(a)(1) provides, in part, as follows:

> The term "false advertising" means advertising, including labeling, of a commodity, or of the kind, character, terms or conditions of any employment opportunity if such advertising is misleading in a material respect. In determining whether any advertising is misleading, there shall be taken into account (among other things) not only representations made by statement, word, design, device, sound or any combination thereof, but also the extent to which the advertising fails to reveal facts material in the light of such representations with respect to the commodity or employment to which the advertising relates under the conditions prescribed in said advertisement, or under such conditions as are customary or usual.

169. Defendant made statements and omissions that were untrue or misleading and disseminated the misleading statements in New York. Defendant disseminated such statements and omissions through advertising, marketing, policies, and other publications. Defendant knew

or through the exercise of reasonable care should have known that such statements and omissions were untrue and misleading.

170. Defendant's security and privacy representations contain untrue and materially misleading statements and omissions regarding the adequacy of Defendant's security and privacy measures.

171. Defendant made numerous material and affirmative misrepresentations and omissions of fact with intent to mislead and deceive concerning Defendant's ability to safeguard Plaintiffs' and Class Members' PII. Specifically, Defendant intentionally concealed and suppressed material facts concerning the identification of the Data Breach of Plaintiffs' and Class Members' PII, the scope of the Data Breach, and the reasons for the Data Breach. Defendant knew, based on its own investigations, that the Data Breach occurred and impacted the PII of hundreds of individuals. Defendant intentionally and grossly defrauded Plaintiffs and Class Members about the security of their PII in Defendant's systems.

172. Defendant made untrue and misleading statements and representations willfully, wantonly, and with reckless disregard for the truth.

173. Defendant's conduct constitutes multiple, separate violations of N.Y. Gen. Bus. Law § 350.

174. Defendant's material misrepresentations were substantially uniform in content, presentation, and impact upon consumers at large. Moreover, all individuals seeking educational services were exposed, and continue to be exposed, to Defendant's material misrepresentations and omissions.

175. Defendant's violations present a continuing risk to Plaintiffs and Class Members. Defendant's deceptive acts and practices affect the public interest.

176. Plaintiffs and Class Members have suffered injury-in-fact and/or actual damages and ascertainable loss as a direct and proximate result of the Defendant's violation.

177. Plaintiffs and Class Members seek monetary relief against Defendant measured as the greater of (i) actual damages in an amount to be determined at trial, and (ii) statutory damages in the amount of $500 for each Class Member, and because Defendant's conduct was committed willingly and knowingly, Class Members are entitled to recover three times actual damages, up to $10,000. Plaintiffs and Class Members also seek an order enjoining Defendant's false advertising, attorneys' fees, and any other just and proper relief under N.Y. Gen. Bus. Law § 350.

COUNT V
VIOLATIONS OF THE NEW YORK DECEPTIVE SALES PRACTICE ACT
New York Gen. Bus. Law § 899-aa
(On behalf of Plaintiffs and the Class against Defendant)

178. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

179. Defendant is a business that owns, or licenses computerized data as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a).

180. Defendant is subject to N.Y. Gen. Bus. Law §§ 899-aa (2) and (3) because Defendant maintains computerized data that includes Plaintiffs' and Class Members' PII which Defendant does not own.

181. Plaintiffs' and Class Members' PII includes information protected and covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

182. Defendant engaged in deceptive, unfair, and unlawful trade acts and practices by failing to reasonably safeguard Plaintiffs' and Class Members' PII, failing to prevent the Data Breach, and failing to mitigate the effects of the Data Breach.

183. Pursuant to this statute, Defendant is required to give immediate notice of a breach of a data system to the owners of PII. Defendant does not own the data that was subject to the Data Breach. Thus, Defendant was required to give immediate notice of the Data Breach to Plaintiffs and Class Members within thirty (30) days of discovery of the Data Breach.

184. Pursuant to this statute, Defendant is required to sufficiently notify Plaintiffs and Class Members if it discovers a security breach or receives notice of a security breach which may compromise PII in the most expedient time possible without unreasonable delay.

185. Defendant failed to timely or sufficiently disclose the Data Breach, a security breach, in violation of N.Y. Gen. Bus. Law §§ 899-aa.

186. As a direct and proximate result of Defendant's violations of N.Y. Gen. Bus. Law §§ 899-aa, Plaintiffs and Class Members suffered damages, including: (i) theft of their PII, which includes highly sensitive medical information; (ii) imminent injury from identity theft; (iii) inability to mitigate the risks of identity theft and fraud due to Defendant's untimely disclosures of the Data Breach; (iv) loss of privacy; (v) the payment of costs to remedy or mitigate the effects of the Data Breach, including, but not limited to, payment for credit monitoring services.

187. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, pray for relief and judgment against Defendant as follows:

a. An order declaring this action to be a proper class action, appointing Plaintiffs as Class Representatives and their counsel undersigned as Class Counsel, and requiring Defendant to bear the costs of class notice;

b. An order enjoining Defendant from inadequately safeguarding the PII that remain in its possession, custody, and control;

c. An order requiring Defendant to develop and implement reasonable security and privacy measures, commensurate with the highly sensitive PII it stores, in accordance with governing legal and industry standards;

d. An order requiring Defendant to engage in a corrective or remedial advertising campaign to alert users and consumers about the specific vulnerabilities in its security and privacy systems, and the steps being taken to remediate those vulnerabilities;

e. An order awarding declaratory relief, and any further retrospective or prospective injunctive relief permitted by law or equity, including enjoining Defendant from continuing the negligent and unlawful practices alleged herein, and injunctive relief to remedy Defendant's past conduct;

f. An order requiring Defendant to pay restitution to restore all funds acquired by means of any act or practice declared by this Court to be an unlawful, unfair, or fraudulent business act or practice, untrue or misleading advertising, or a violation of law, plus pre- and post-judgment interest thereon;

g. An order requiring Defendant to disgorge or return all monies, revenues, and profits obtained by means of any wrongful or unlawful act or practice;

h. Awarding Plaintiffs and the Class compensatory damages, in an amount exceeding $5,000,000, to be determined at trial;

i. Awarding Plaintiffs and the Class appropriate relief, including actual and statutory damages;

j. Awarding Plaintiffs and the Class punitive damages;

k. Awarding Plaintiffs and the Class the costs of prosecuting this action, including expert witness fees;

l. Awarding Plaintiffs and the Class reasonable attorneys' fees and costs as allowable by law;

m. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest; and

n. Granting any other relief as this Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: January 17, 2025

Respectfully submitted,

/s/Michael P. Canty
LABATON SUCHAROW LLP
Michael P. Canty
Carol C. Villegas
Danielle Izzo
Michael Hotz
140 Broadway
New York, New York 10005
Telephone: (212) 907-0700
Facsimile: (212) 818-0477
mcanty@labaton.com
cvillegas@labaton.com
dizzo@labaton.com
mhotz@labaton.com

Counsel for Plaintiffs and the Proposed Class